



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/756,444	01/12/2004	Balaji Vembu	42P18507	2132
59796	7590	12/06/2007	[REDACTED]	[REDACTED]
INTEL CORPORATION			EXAMINER	
c/o INTELLEVATE, LLC			PERUNGAVOOR, VENKATANARAY	
P.O. BOX 52050			[REDACTED]	[REDACTED]
MINNEAPOLIS, MN 55402			ART UNIT	PAPER NUMBER
			2132	
			[REDACTED]	[REDACTED]
			MAIL DATE	DELIVERY MODE
			12/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/756,444	VEMBU, BALAJI	
	Examiner	Art Unit	
	Venkat Perungavoor	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 05 November 2007.
- 2a) This action is **FINAL**. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-21 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-21 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO/SB/08)
 Paper No(s)/Mail Date _____
- 4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____
- 5) Notice of Informal Patent Application
 6) Other: _____

DETAILED ACTION

Response to Arguments

Applicant's arguments filed 11/5/2007 have been fully considered but they are not persuasive.

The Applicant argues independent claims 1, 10 and 18. The Examiner will rebut the arguments here.

Regarding claims 1, 10, and 18, the Applicant argues that Hillier nor Lyson disclose the third entity encrypting the first key(recipient's key) using second key(originator's key) and further decrypting the first key using the second key.

Hillier discloses the third party(3rd party processor) communicating with the originator and the recipient thorough notifications and replies see Fig.1 item 24, 22. And further discloses the third party decrypting of ciphertext using received package containing keys see Col 8 Ln 20-31. And Lyson discloses the re-encrypting of received package using the see Fig. 2 item 54 & Col 5 Ln 40-51. This is done by re-encrypting by a third party(new user) using keys from the previous encryptions see Col 6 Ln 17-49.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:
 - (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a

person having ordinary skill in the art to which said subject matter pertains.
Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-5,7-13, 16, are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 7142676 to Hillier et al.(hereinafter Hillier) in view of US Patent 6336121 to Lyson et al.(hereinafter Lyson) further in view of US Patent 6256733 to Thakkar et al.(hereinafter Thakkar).
3. Regarding Claim 1, 10, Hillier discloses the first entity(originator processor) having associated with a key(KS1) , second entity(recipient processor) associated with a key(2ndEPuK) and third entity(third party processor) associated with a key(3rdEPuk) see Fig. 1 & Col 5 Ln 41- Col 6 Ln 13; decrypting of keys(KS2, KS, KS1) using third party's private keys see Col 6 Ln 3-13 & Col 7 Ln 5-20. But fails to explicitly disclose the encrypting the first key by the second key and another entity obtaining this key and further decrypting the first key encrypted by second key. However, Lyson discloses the re-encrypting the captured data and further of a requesting entity decrypting the encrypted key to obtain key see Fig. 3 item 70, 72, 74 & Col 5 Ln 40-51 & Col 6 Ln 19-23. It would be obvious to one having ordinary skill in the art at the time of the invention to include the re-encrypting of captured data and decrypting to obtain key in the invention of Hillier in order to have a reduced number of keys as taught in Lyson see Col 2 Ln 39-44. Neither Hillier nor Lyson explicitly disclose the encrypting of keys using the public key of an entity. However, Thakkar discloses the encrypting of keys using the public key see Col 1 Ln 37-53. It would be obvious to one having ordinary skill in the art at the time of the invention to include the use

of encrypting key using public keys in the invention of Hillier in order to provide for signature verification using publicly available data as taught in Thakkar see Col 1 Ln 36-46.

4. Regarding Claim 2, 16, Hillier discloses direct communication between originator and recipient after connection see Col 4 Ln 23-27.
5. Regarding Claim 3-4, 11-12, Hillier discloses the processor, which includes an graphics device and application program see Fig. 1 item 12, 14.
6. Regarding Claim 5, 13, Hillier discloses the trust third party see Col 2 Ln 16-20.
7. Claims 6, 14-15, 17, 20, are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 7142676 to Hillier et al.(hereinafter Hillier) in view of US Patent 6336121 to Lyson et al.(hereinafter Lyson) further in view of US Patent 2003/0194093 to Evans et al.(hereinafter Evans).
8. Regarding Claim 6, 15, Hillier nor Lyson explicitly disclose the pseudo-randomly generated keys. However, Evans discloses the pseudo-randomly generated keys see Par. 0067. It would be obvious to one having ordinary skill in the art at the time of the invention to include the pseudo-randomly generated keys in the invention of Hillier in order to have key that is never revealed as taught in Evans see Par. 0067 & Par. 0068.

9. Regarding Claim 14, 17, 20, Hillier nor Lyson explicitly disclose registers for storing keys or input/output pin dedicated to use by first entity. However, Evans discloses the registers for storing keys see Par. 0028 and input/output pin dedicated to use by first entity see Par. 0031 & Par. 0029. It would be obvious to one having ordinary skill in the art at the time of the invention to include registers in the invention of Hiller in order to have a unit for storing keys as taught in Evans see Par. 0029.
10. Claims 18-19, 21, are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 7142676 to Hillier et al.(hereinafter Hillier) in view of US Patent 6336121 to Lyson et al.(hereinafter Lyson) further in view of US Patent 6256733 to Thakkar et al.(hereinafter Thakkar) further in view of US Patent 2003/0194093 to Evans et al.(hereinafter Evans).
11. Regarding Claim 18, Hillier discloses the first entity(originator processor) having associated with a key(KS1) , second entity(recipient processor) associated with a key(2ndEPuK) and third entity(third party processor) associated with a key(3rdEPuk) see Fig. 1 & Col 5 Ln 41- Col 6 Ln 13; decrypting of keys(KS2, KS, KS1) using third party's private keys see Col 6 Ln 3-13 & Col 7 Ln 5-20. But fails to explicitly disclose the encrypting the first key by the second key and another entity obtaining this key and further decrypting the first key encrypted by second key. However, Lyson discloses the re-encrypting the captured data and further of a requesting entity decrypting the encrypted key to obtain key see Fig. 3 item 70, 72, 74 & Col 5 Ln 40-51 & Col 6 Ln 19-23. It would be obvious to one having ordinary skill in the art at the time of the invention to include the re-encrypting of captured data and

decrypting to obtain key in the invention of Hillier in order to have a reduced number of keys as taught in Lyson see Col 2 Ln 39-44. Neither Hillier nor Lyson explicitly disclose the encrypting of keys using the public key of an entity. However, Thakkar discloses the encrypting of keys using the public key see Col 1 Ln 37-53. It would be obvious to one having ordinary skill in the art at the time of the invention to include the use of encrypting key using public keys in the invention of Hillier in order to provide for signature verification using publicly available data as taught in Thakkar see Col 1 Ln 36-46. Further yet, Hillier nor Lyson nor Thakkar explicitly disclose the pseudo-randomly generated keys. However, Evans discloses the pseudo-randomly generated keys see Par. 0067. It would be obvious to one having ordinary skill in the art at the time of the invention to include the pseudo-randomly generated keys in the invention of Hillier in order to have key that is never revealed as taught in Evans see Par. 0067 & Par. 0068. Further, Hillier nor Lyson explicitly disclose registers for storing keys or input/output pin dedicated to use by first entity. However, Evans discloses the registers for storing keys see Par. 0028 and input/output pin dedicated to use by first entity see Par. 0031 & Par. 0029. It would be obvious to one having ordinary skill in the art at the time of the invention to include registers in the invention of Hiller in order to have a unit for storing keys as taught in Evans see Par. 0029.

12. Regarding Claim 19, Hillier discloses the signal the start of key exchange see Fig. 3a item 42.

13. Regarding Claim 21, Hillier discloses the decrypting the encrypted content see Fig. 4 item 55.

Conclusion

- 14. THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.
15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Venkat Perungavoor whose telephone number is 571-272-7213. The examiner can normally be reached on 8:30-5:00. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Application/Control Number:
10/756,444
Art Unit: 2132

Page 8

16. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/VP/
Venkat Perungavoor
Examiner
Art Unit 2132
December 5, 2007


GILBERTO BARRON 
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100